



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,044	02/14/2002	Kang Chun Un	Q67312	7599

7590 07/13/2007
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3213

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

07/13/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/074,044	UN, KANG CHUN
	Examiner Samson B. Lemma	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 06 November 2006.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-8 and 14 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-8 and 14 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

1. This office action is in reply to Response to Election/Restriction filed on November 07, 2006.
2. Applicant's election without traverse of Group I (claims 1-8 and 14 in the reply filed on November 07, 2006 is acknowledged. Thus claims 1-8 and 14 are pending/examined.

Response to Arguments

3. Applicant's arguments/remarks filed on June 22, 2006 have been fully considered and they are not persuasive.

Applicant argued that the combination of **Scott and Nagashima** (the references on the record) does not teach or suggest some of the limitation enclosed in the independent claims.

Applicant wrote the following in support of his argument.

"Scott discloses "storing an ID code associated only with a portable registered device controlled by the registered person" Scott, c. 4/11.8-9. It also discloses that "the encrypted data [includes] a synchronization counter associated with the user device." Id., c. 4/11.28-29. And that "the units are manufactured with unique ID codes and private keys." Id., c. 5/11.60-61.

However, Scott does not appear to disclose that the ID code of a user device can change. Instead, the ID code appears to be fixed for a given user device. Thus, to the extent that the ID code for a given user device of Scott corresponds to important information, that important information does not change. And, as a result, Scott doesn't disclose that the synchronization counter associated with the specific user device changes when a portion of the important information for that user device is updated (i.e., it doesn't disclose "storing synchronizing information, which changes when a portion of the important information is updated, in the

database together with the important information, and encrypting the synchronizing information"."

Furthermore, Applicant wrote the following in support of his argument.

"Nagashima attempts to store and securely manage secret key K as its important data. And Nagashima attempts to store in a plurality of second apparatuses at least one piece of partial information Kli (I = 1, 2, ...) related to its important data, not any synchronizing information. Thus, Applicant submits that Nagashima does not disclose "storing synchronizing information, which changes when a portion of the important information is updated, in the database together with the important information, and encrypting the synchronizing information", "distributively storing the encrypted synchronizing information in a plurality of predetermined places", or "combining and decrypting the synchronizing information stored in the predetermined places and determining whether the combined synchronizing information is identical to the synchronizing information stored in the database"."

Examiner disagrees with this argument.

Examiner would point out that the user code and the corresponding synchronizing information is different for each PID and changes/updates when the PID (portable personal identification device Changes which means when the ID code changes because each PID has its own ID code.

For instance, on column 8, lines 7-14, the following has been disclosed.

" Encoder 23A includes an **ID code, which may be a serial number of encoder 23 or PID 6A. Encoder 23A also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system 4A must "learn" the **ID code and the synchronization counter for each PID 6A which is used to access a function of host system 4A**. Host system 4A must also know the encryption key."**

Therefore the ID code which meets the limitation of important information is stored as indicated on column 4, lines 32-33, together with the synchronization counter which meets the limitation of synchronizing information and together they are stored in the host system. The storing of synchronizing counter is explained on column 12, lines 52-53 and also taught on column 8, lines 7-14 in the host system 4A or on column 4, lines 38-39, "synchronization counter of the registered device". For every user this synchronizing information changes when the PID changes or when the ID code changes because each and every PID has its own unique ID code otherwise the host won't be able to differentiate one PID from another and accessing the host system will not function properly. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In order to show how each and every limitation of the independent claims are disclosed by the combination of references on the record, the examiner would point out the following,

As per claims 1, Scott, the primary reference on the record discloses a method for storing and securely managing important information for a user in a database, [Column 4, lines 7-9] (registering a person with the host facility by storing an ID code associated only with portable registered device controlled by the registered person. An ID code meets the limitation of the important information and storing an ID code in host facility meets the limitation of storing and securely managing important information for a user in a database) comprising:

Storing synchronizing information, [Column 12, lines 52-53] (stored synchronization counter information in memory) which changes when a portion of the important information is updated, in the database together with the important information, [column 4, lines 32-33 and column 8, lines 7-14] (stored ID code) (The ID code which meets the limitation of important information is stored as indicated on column 4, lines 32-33, together with the synchronization counter which meets the limitation of synchronizing information. The storing of synchronizing counter is explained on column 12, lines 52-53 and inherently taught on column 4, lines 38-39, "synchronization counter of the registered device". This synchronizing information changes when the ID code changes and on column 8, lines 7-14, the following has been disclosed. "Encoder 23A includes an **ID code, which may be a serial number of encoder 23 or PID 6A. Encoder 23A also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system 4A must "learn" the **ID code and the synchronization counter for each PID 6A which is used to access a function of host system 4A**. Host system 4A must also know the encryption key." Therefore the ID code which meets the limitation of important information is stored as indicated on column 4, lines 32-33, together with the synchronization counter which meets the limitation of synchronizing information and together they are stored in the host system. The storing of synchronizing counter is explained on column 12, lines 52-53 and also taught on column 8, lines 7-14 in the host system 4A or on column 4, lines 38-39, "synchronization counter of the registered device". For every user this synchronizing information changes when the PID changes or when the ID code changes because each and every PID has its own unique ID code otherwise the host won't be able to differentiate one PID from another and accessing the host system will not function properly.)**

and

encrypting the synchronizing information; [column 4, lines 28-29]

(encrypting data including a synchronization counter.)

Sending the encrypted synchronizing information to a predetermined place/s; [Column 4, lines 24-29] (The access signal which includes the synchronization counter/synchronizing information is encrypted and sent to the host facility meets the limitation of predetermined place/s. This inherently includes storing the encrypted synchronization counter for a certain period of time/temporarily at the host facility before the synchronization counter is decrypted).

Decrypting the synchronizing information in the predetermined places and determining whether the decrypted synchronizing information is identical to the synchronizing information stored in the database. [Column 4, lines 35-42 and column 12, lines 50-59]

Scott does not explicitly disclose,

Distributively storing data in a plurality of predetermined places and combining the data and decrypting the data.

However, in the same field of endeavor, **Nagashima** discloses

- Storing the key data distributively in a plurality of predetermined places and combining/collecting a predetermined number of pieces of information/data which are distributively stored and perform decryption.[Page 4, lines 9-10]

Though the application has allowable subject matter the independent claim 1 has not yet been written to overcome the ground of the rejection set forth in the previous office action. Therefore the rejection is maintained until applicant amends at least the independent claim without introducing a new matter.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-8 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al (hereinafter referred as **Scott**) (U.S. Patent No. 6,484,260 B1) in view of Nagashima, Takayuki (hereinafter referred as **Nagashima**) (**European patent No. EP 0851629 A2 (Publication date 07/01/1998)**

6. **As per claims 1, Scott, the primary reference on the record discloses a method for storing and securely managing important information for a user in a database, [Column 4, lines 7-9]** (registering a person with the host facility by storing an ID code associated only with portable registered device controlled by the registered person. **An ID code** meets the limitation of the important information and **storing an ID code in host facility** meets the limitation of storing and securely managing important information for a user in a database) **comprising:**

Storing synchronizing information, [Column 12, lines 52-53] (stored synchronization counter information in memory) **which changes when a**

portion of the important information is updated, in the database together with the important information, [column 4, lines 32-33 and column 8, lines 7-14] (stored ID code) (The ID code which meets the limitation of important information is stored as indicated on column 4, lines 32-33, together with the synchronization counter which meets the limitation of synchronizing information. The storing of synchronizing counter is explained on column 12, lines 52-53 and inherently taught on column 4, lines 38-39, "synchronization counter of the registered device". This synchronizing information changes when the ID code changes and on column 8, lines 7-14, the following has been disclosed. "Encoder 23A includes an **ID code**, which may be a serial number of encoder 23 or PID 6A. Encoder 23A also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system 4A must "learn" the **ID code and the synchronization counter for each PID 6A which is used to access a function of host system 4A**. Host system 4A must also know the encryption key." Therefore the ID code which meets the limitation of important information is stored as indicated on column 4, lines 32-33, together with the synchronization counter which meets the limitation of synchronizing information and together they are stored in the host system. The storing of synchronizing counter is explained on column 12, lines 52-53 and also taught on column 8, lines 7-14 in the host system 4A or on column 4, lines 38-39, "synchronization counter of the registered device". For every user this synchronizing information changes when the PID changes or when the ID code changes because each and every PID has its own unique ID code otherwise the host won't be able to differentiate one PID from another and accessing the host system will not function properly.)

and

encrypting the synchronizing information; [column 4, lines 28-29]

(encrypting data including a synchronization counter.)

Sending the encrypted synchronizing information to a predetermined place/s; [Column 4, lines 24-29] (The access signal which includes the synchronization counter/synchronizing information is encrypted and sent to the host facility meets the limitation of predetermined place/s. This inherently includes storing the encrypted synchronization counter for a certain period of time/temporarily at the host facility before the synchronization counter is decrypted).

Decrypting the synchronizing information in the predetermined places and determining whether the decrypted synchronizing information is identical to the synchronizing information stored in the database. [Column 4, lines 35-42 and column 12, lines 50-59]

Scott does not explicitly disclose,

Distributively storing data in a plurality of predetermined places and combining the data and decrypting the data.

However, in the same field of endeavor, **Nagashima** discloses

- Storing the key data distributively in a plurality of predetermined places and combining/collecting a predetermined number of pieces of information/data which are distributively stored and perform decryption.[Page 4, lines 9-10]

Though the application has allowable subject matter the independent claim 1 has not yet been written to overcome the ground of the rejection set forth in the previous office action. Therefore the rejection is maintained until applicant amends at least the independent claim without introducing a new matter.

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of storing data/information distributively on a plurality of predetermined places and combining them and perform decryption as per teachings of **Nagashima** in to the method as taught by Scott in order to securely mange information in database/facility/storage.

7. **As per claim 2 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore **Scott** discloses the method, wherein the encrypting the synchronizing information comprises encrypting key-data used for encrypting and decrypting the synchronizing information. [column 4, lines 28-39 and column 12, lines]

8. **As per claim 3 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore **Nagashima** discloses the method, wherein the distributively storing the encrypted synchronizing information comprises distributively storing key-data in said predetermined places. [Page 4, line 6; figure 1, ref "11b, 11c and 11d]

9. **As per claim 4 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore **Scott** discloses the method, wherein the encrypting the synchronizing information comprises encrypting the updated important information. [Column 4, line 27] (encrypting data includes encrypting the updated important information]

Art Unit: 2132

10. **As per claim 5 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore Scott discloses the method, wherein the encrypting the synchronizing information comprises encrypting key data used for encrypting and decrypting the important information. [column 4, lines 28-39 and column 12, lines]

11. **As per claim 6-7 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore **Nagashima** discloses the method, wherein the distributively storing the encrypted synchronizing information comprises distributively storing the encrypted key-data in predetermined places. [Page 4, lines 4-10, figure 1, ref "11b, 11c and 11d]

12. **As per claim 8 & 14 the combination of Scott and Nagashima** discloses a method for storing and securely managing important information for a user in a database as applied to claims above. Furthermore **Scott** discloses the method, wherein the combining, decrypting and determining step comprises combining and decrypting the important information stored in the predetermined places and determining whether the decrypted important information is identical to the important information stored in the database. [Column 4, lines 24-42 and column 12, lines 50-59]

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2132

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
07/01/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100